ON THE SUM OF TWO INTEGRAL SQUARES IN CERTAIN QUADRATIC FIELDS

DASHENG WEI

Abstract

We propose a method for determining which integers can be written as a sum of two integral squares for certain quadratic fields.

MSC classification : 11E12;11D09

Keywords : integral points, ring class field, reciprocity law.

Introduction

It is significantly more difficult to study sums of two integral squares over algebraic number fields than that over $\mathbb{Z}$. From nowadays point of view, Fermat-Gauss' theorem about sums of two squares over $\mathbb{Z}$ is a purely local problem. However such question is a global problem over algebraic number fields, even quadratic fields since the class number of number fields is involved. There are only a few results about the question for general algebraic number fields F. Niven studied the problem for $F = \mathbb{Q}(\sqrt{-1})$ in [12]. This case is very special since the binary quadratic form $x^2 + y^2$ is hyperbolic over $\mathbb{Q}(\sqrt{-1})$. Nagell further studied the problem for $F = \mathbb{Q}(\sqrt{d})$ when d is one of the following twenty integers:

$$\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 19, \pm 43, \pm 67, \pm 163$$

in [9] and [10]. His method follows Gauss' original idea and essentially depends on the fact that the class number of $\mathbb{Q}(\sqrt{d}, \sqrt{-d})$ is 1 when d is one of the above integers. Obviously this method can not apply for general algebraic number fields.

Recently Harari (in [5]) proved that the Brauer-Manin obstruction to the existence of an integral point is the only obstruction for an integral model of a principal homogenous space of tori. However, the Brauer group is infinite. One cannot use these results to determine the existence of integral points on a specific example. Fei Xu and the author gave another proof of the result in [21] and [22]. In this paper we apply the method in [21] for the sum of two squares over quadratic fields.

It should be pointed out that the method in [21] only produces the idelic class groups of $F(\sqrt{-1})$ for solving the problem of sum of two squares. And these idelic class groups are not unique. In order to get the explicit conditions for the sum of two squares, one needs further to construct the explicit abelian extensions of $F(\sqrt{-1})$ corresponding to the idelic class groups by the class field theory. Such explicit construction is a wide open problem (Hilbert's 12-th problem) in general but ad hoc methods.

Date: May 6, 2010.

Notation and terminology are standard if not explained. Let F be a number field, $\mathfrak{o}_F$ the ring of integers of F, Ω_F the set of all primes in F and ∞ the set of all infinite primes in F. For simplicity, we write $\mathfrak{p} < \infty$ for $\mathfrak{p} \in \Omega_F \setminus \infty$. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$ and $\mathfrak{o}_{F_\mathfrak{p}}$ be the local completion of $\mathfrak{o}_F$ at $\mathfrak{p}$ for each $\mathfrak{p} \in \Omega_F$. Write $\mathfrak{o}_{F_\mathfrak{p}} = F_\mathfrak{p}$ for $\mathfrak{p} \in \infty$. We also denote the adele ring (resp. the idele ring) of F by $\mathbb{A}_F$ (resp. $\mathbb{I}_F$).

Suppose that -1 is not a square in F. Let $E = F(\sqrt{-1})$. Let $\mathbf{X}_\alpha$ denote the affine scheme over $\mathfrak{o}_F$ defined by the equation $x^2 + y^2 = \alpha$ for a non-zero integer $\alpha \in \mathfrak{o}_F$. The equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$. Let $X_\alpha = \mathbf{X}_\alpha \times_{\mathfrak{o}_F} F$. Obviously $f = x + y\sqrt{-1}$ is an invertible function on $X_\alpha \otimes_F E$. And f induces a natural map

$$f_E : \quad X_\alpha(\mathbb{A}_F) \to \mathbb{I}_E.$$

The restriction to $X_\alpha(F_\mathfrak{p})$ of f_E can be defined by

$$f_E[(x_\mathfrak{p}, y_\mathfrak{p})] = \begin{cases} (x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, x_\mathfrak{p} - y_\mathfrak{p}\sqrt{-1}) & \text{if } \mathfrak{p} \text{ splits in } E/F, \\ x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1} & \text{otherwise.} \end{cases}$$

Definition 0.1. Let $K_1, \cdots, K_n$ be finite abelian extensions over E. Let

$$\psi_{K_i/E} : \mathbb{I}_E \to Gal(K_i/E) \text{ for } 1 \leq i \leq n$$

be the Artin map. We say that α satisfies the Artin condition of $K_1, \cdots, K_n$ if there is

$$\prod_{\mathfrak{p} \leq \infty} (x_\mathfrak{p}, y_\mathfrak{p}) \in \prod_{\mathfrak{p} \leq \infty} \mathbf{X}_\alpha(\mathfrak{o}_{F_\mathfrak{p}})$$

such that

$$\psi_{K_i/E}(f_E[\prod_{\mathfrak{p} \leq \infty} (x_\mathfrak{p}, y_\mathfrak{p})]) = 1_i \text{ for } i = 1, \cdots, n$$

where 1_i is the identity element of $Gal(K_i/E)$.

By the class field theory, it is a necessary condition for $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$ that α satisfies the Artin condition of $K_1, \cdots, K_n$. There exists a (not unique) finite abelian extension K/E independent on α, such that the Artin condition of K is also sufficient for $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$ (Corollary 2.18 in [21]). Let $d \geq 2$ be a positive square-free integer and $F = \mathbb{Q}(\sqrt{-d})$. Then the field K closely depends on the (local and global) solvability of the following equation

$$x^2 + y^2 = -1. \tag{0.1}$$

Let $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$ and H_L be the ring class field corresponding to the order L. For example, the Artin condition of H_L is sufficient if $F = \mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$ with p prime (Theorem 0.3 in [20]). And the following result can be found in [20] (Proposition 1.1).

Proposition 0.2. *Suppose one of the following conditions holds:*

(1) The equation (0.1) has an integral solution in $\mathfrak{o}_F$.

(2) The equation (0.1) has no local integral solutions at a place of F.

Then the equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of H_L.

Therefore we only need to consider the case that the two conditions in Proposition 0.2 don't hold. For this case the Arin condition of H_L must not be sufficient. In general the question will be very complicated. We can not expect to construct a field K generally, such that the Artin condition of K is sufficient.

The following result is well-known (Satz 2, [14]): the equation (0.1) is solvable over $\mathfrak{o}_F$ if and only if the equation

$$x^2 - dy^2 = -\gamma(d) \tag{0.2}$$

is solvable over $\mathbb{Z}$, where

$$\gamma(d) = \begin{cases} 1 & \text{if } d \not\equiv -1 \mod 4 \\ 2 & \text{if } d \equiv -1 \mod 4. \end{cases}$$

In this paper, we will consider the case that the equation (0.1) is solvable over $\mathfrak{o}_{F_\mathfrak{p}}$ for any $\mathfrak{p} \in \Omega_F$ and the equation (0.2) is not solvable over $\mathbb{Z}_p$ for some prime p. It is easy to see that the two conditions in Proposition 0.2 don't hold for this case. Let

$$C = \{(d,p) | d \text{ is a square-free positive integer and } p \mid d \text{ with } p \text{ prime}\}$$
$$D_1 = \{(d,p) \in C | d \not\equiv -1 \mod 8, p \equiv -1 \mod 8\}$$
$$D_2 = \{(d,p) \in C | d \equiv 1, 2 \mod 4, p \equiv 3 \mod 8\}$$
$$D_3 = \{(d,p) \in C | d \equiv 3 \mod 8, p \equiv 5 \mod 8\}$$

Denote

$$D = D_1 \cup D_2 \cup D_3.$$

We say that $d \in D$ (or D_i) if there is a prime p such that $(d,p) \in D$ (or D_i). It is easy to verify that the equation (0.1) is solvable over $\mathfrak{o}_{F_\mathfrak{p}}$ for any $\mathfrak{p} \in \Omega_F$ and the equation (0.2) is not solvable over $\mathbb{Z}_p$ for some prime p if and only if $d \in D$. In this paper, we mainly prove the following result.

Theorem 0.3. *Let $(d,p) \in D$ and $F = \mathbb{Q}(\sqrt{-d})$. Then the diophantine equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of Θ and H_L,where $\Theta = E(\sqrt[4]{p})$.*

Sums of two integral squares over real quadratic fields is more complicated than that over imaginary quadratic fields, since there are more units in real quadratic fields. In this paper, we also obtain a result about real quadratic fields.

Theorem 0.4. *Let p be a prime and $F = \mathbb{Q}(\sqrt{2p})$. If $p \equiv 3 \mod 8$, then the diophantine equation $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of Θ and H_L, where $\Theta = E(\sqrt[4]{2})$.*

As application, we explicitly determine which integers can be written as a sum of two integral squares for the two quadratic fields $\mathbb{Q}(\sqrt{\pm 6})$, and $\mathbb{Q}(\sqrt{\pm 6})$ are the fields with the smallest $|d|$ that the Artin condition of H_L is not sufficient for $\mathbb{Q}(\sqrt{d})$.

1. The sum of two squares in imaginary quadratic fields

Let F be an algebraic number field and -1 is not a square in F. Let $E = F(\sqrt{-1})$ and let T be the torus $R^1_{E/F}(\mathbb{G}_m) = \mathrm{Ker}[R_{E/F}(\mathbb{G}_{m,E}) \to \mathbb{G}_{m,F}]$, here R denotes the Weil's restriction (see [8]). Denote λ to be the embedding from T to $R_{E/F}(\mathbb{G}_{m,E})$. Obviously λ induces a natural group homomorphism

$$\lambda_E : \quad T(\mathbb{A}_F) \to \mathbb{I}_E.$$

Let $\mathbf{X}_\alpha$ denote the affine scheme over $\mathfrak{o}_F$ defined by $x^2 + y^2 = \alpha$ for a non-zero integer $\alpha \in \mathfrak{o}_F$. Let $\mathbf{T}$ be the group scheme over $\mathfrak{o}_F$ defined by $x^2 + y^2 = 1$ and let $T = \mathbf{T} \times_{\mathfrak{o}_F} F$. The generic fiber of $\mathbf{X}_\alpha$ is a principal homogenous space of the torus T. Since $\mathbf{T}$ is separated over $\mathfrak{o}_F$, we can view $\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$ as a subgroup of $T(F_\mathfrak{p})$. The following result can be founded in [21] (Corollary 2.20).

Proposition 1.1. *Let K_1/E and K_2/E be finite abelian extensions such that the group homomorphism $\widetilde{\lambda}_E$ induced by λ_E*

$$\widetilde{\lambda}_E : {}^{T(\mathbb{A}_F)}\big/_{T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})} \longrightarrow {}^{\mathbb{I}_E}\big/_{E^*N_{K_1/E}(\mathbb{I}_{K_1})} \times {}^{\mathbb{I}_E}\big/_{E^*N_{K_2/E}(\mathbb{I}_{K_2})}$$

is well-defined and injective, where well-defined means

$$\lambda_E(T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})) \subset (E^*N_{K_1/E}(\mathbb{I}_{K_1})) \cap (E^*N_{K_2/E}(\mathbb{I}_{K_2})).$$

Then $\mathbf{X}_\alpha(\mathfrak{o}_F) \neq \emptyset$ if and only if α satisfies the Artin condition of K_1 and K_2.

Let $d \geq 2$ be a square-free positive integer. Let $F = \mathbb{Q}(\sqrt{-d})$, $\mathfrak{o}_F$ be the ring of integers of F and $E = F(\sqrt{-1})$. In the rest of this section F is always an imaginary quadratic field. One takes the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$ inside E. Let H_L be the ring class field corresponding to the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$. Recall some notations:

$$\begin{aligned}
C &= \{(d,p) | d \text{ is a square-free positive integer and } p \mid d \text{ with } p \text{ prime}\}\\
D_1 &= \{(d,p) \in C | d \not\equiv -1 \mod 8, p \equiv -1 \mod 8\}\\
D_2 &= \{(d,p) \in C | d \equiv 1,2 \mod 4, p \equiv 3 \mod 8\}\\
D_3 &= \{(d,p) \in C | d \equiv 3 \mod 8, p \equiv 5 \mod 8\}.
\end{aligned}$$

Note that $p \equiv 3 \mod 4$ if $(d,p) \in D_1 \cup D_2$.

Proposition 1.2. *Suppose $(d,p) \in D_1 \cup D_2$ and $F = \mathbb{Q}(\sqrt{-d})$. Let $(x_\mathfrak{p}, y_\mathfrak{p}) \in \mathfrak{o}_{F_\mathfrak{p}} \times \mathfrak{o}_{F_\mathfrak{p}}$, then the 4-th Hilbert symbol*

$$\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v}\right)_4 = \begin{cases} 1 & \text{if } x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = 1 \\ -1 & \text{if } x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = -1, \end{cases}$$

where v and $\mathfrak{p}$ are respectively the unique place of E and F above p.

Proof. The Hilbert symbol

$$\begin{aligned}
\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v}\right)_4 &= \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, -d}{v}\right)_4 \cdot \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, -d/p}{v}\right)_4^{-1}\\
&= \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, -d}{v}\right)_4 \cdot 1 = \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, \sqrt{-d}}{v}\right)\\
&= \left(\frac{\pm 1, p}{p}\right) = \pm 1,
\end{aligned}$$

where the second equation holds since $E(\sqrt[4]{-d/p})/E$ is unramified at v. □

Proposition 1.3. *Suppose $(d,p) \in D_1 \cup D_2$ and $F = \mathbb{Q}(\sqrt{-d})$. If $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, then*

$$\prod_{v|2}\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v}\right)_4 = 1$$

where $v \in \Omega_E$ and $\mathfrak{p}$ is the unique place of F above 2.

The proposition follows from the series of lemmas.

Lemma 1.4. *Let $d \not\equiv -1 \mod 8$ and $l \equiv -1 \mod 8$. Let $F = \mathbb{Q}(\sqrt{-d})$. If $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $F_\mathfrak{p}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, then*

$$\prod_{v|2} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v} \right)_4 = 1$$

where $v \in \Omega_E$ and $\mathfrak{p}$ is the unique place of F above 2.

Proof. The extension $E(\sqrt{l})/E$ is split over v. And

$$\sqrt{l} = s\sqrt{-1} = (2\sqrt{-1}) \cdot \frac{s}{2} = (1+\sqrt{-1})^2 \frac{2s}{2^2},$$

where $s^2 = -l$ and $s \in \mathbb{Z}_2^\times$. For any $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $F_\mathfrak{p}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, we have

$$\begin{aligned} \prod_{v|2} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v} \right)_4 &= \prod_{v|2} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, \sqrt{l}}{v} \right) = \prod_{v|2} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, 2s}{v} \right) \\ &= \left(\frac{\pm 1, 2s}{\mathfrak{p}} \right) = 1. \end{aligned}$$

□

Proposition 1.3 for the case $(d,p) \in D_1$ follows from the above lemma. The following two lemmas deal with the case $(d,p) \in D_2$.

Lemma 1.5. *Let $d \equiv 1 \mod 4$ and $l \equiv 3 \mod 8$. Let $F = \mathbb{Q}(\sqrt{-d})$. If $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, then*

$$\prod_{v|2} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v} \right)_4 = 1$$

where $v \in \Omega_E$ and $\mathfrak{p}$ is the unique place of F above 2.

Proof. (1) If $d \equiv 5 \mod 8$, then $F = \mathbb{Q}(\sqrt{-d}) = \mathbb{Q}(\sqrt{l})$. And v is the unique place of E above 2. For any $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $F_\mathfrak{p}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, we have

$$\begin{aligned} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v} \right)_4 &= \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, \sqrt{l}}{v} \right) \\ &= \left(\frac{\pm 1, \sqrt{l}}{\mathfrak{p}} \right) = \left(\frac{\pm 1, -l}{2} \right) \\ &= 1. \end{aligned}$$

(2) If $d \equiv 1 \mod 8$, then E/F is split over $\mathfrak{p}$. For any $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, we have

$$\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v} \right) = 1$$

since $E(\sqrt{l})/E$ is unramified at any place v of E above 2. So we have

$$\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v} \right)_4 = \pm 1.$$

Therefore

$$\prod_{v|2}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4=\left(\frac{(x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1})(x_\mathfrak{p}-y_\mathfrak{p}\sqrt{-1}),l}{\mathfrak{p}}\right)_4$$
$$=\begin{cases}1 & \text{if } x_\mathfrak{p}^2+y_\mathfrak{p}^2=1\\ \left(\frac{-1,l}{\mathfrak{p}}\right)_4=\left(\frac{\sqrt{-1},l}{\mathfrak{p}}\right)=1 & \text{if } x_\mathfrak{p}^2+y_\mathfrak{p}^2=-1.\end{cases}$$

□

Lemma 1.6. *Let $d\equiv 2 \mod 4$ and $l\equiv\pm 3 \mod 8$. Let $F=\mathbb{Q}(\sqrt{-d})$. If $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2+y_\mathfrak{p}^2=\pm 1$, then*

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4=1$$

where v and $\mathfrak{p}$ are respectively the unique place of E and F above 2.

Proof. (1) First we will prove that $\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4=1$ for any $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ that satisfy $x_\mathfrak{p}^2+y_\mathfrak{p}^2=1$.

By Hilbert 90, there exists $\beta\in E_v^*$ such that $x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1}=\sigma(\beta)/\beta$, where σ is the non-trivial element of $Gal(E_v/F_\mathfrak{p})$. Let $\beta=a+b\sqrt{-1}$ and we can choose β such that $a,b\in\mathfrak{o}_{F_\mathfrak{p}}$ and a or b is a unit. Denote $\kappa=a^2+b^2$.

Assume that $ord_\mathfrak{p}(\kappa)$ is odd. The equation $x^2+y^2=\kappa$ is not solvable over $\mathfrak{o}_{F_\mathfrak{p}}$ if $ord_\mathfrak{p}(\kappa)=1$ (by Theorem 1 in [6]). Therefore $ord_\mathfrak{p}(\kappa)\geq 3$. We have $a,b\in\mathfrak{o}_{F_p}^\times$ and

$$\beta/\sigma(\beta)=(a^2-b^2-2ab\sqrt{-1})\kappa^{-1}=1-2\kappa^{-1}b^2-2\kappa^{-1}ab\sqrt{-1}.$$

Since $ord_\mathfrak{p}(\kappa)\geq 3$ and $a,b\in\mathfrak{o}_{F_\mathfrak{p}}^\times$, one has

$$2\kappa^{-1}b^2,2\kappa^{-1}ab\notin\mathfrak{o}_{F_\mathfrak{p}}.$$

So $\beta/\sigma(\beta)\notin\mathfrak{o}_{F_\mathfrak{p}}+\mathfrak{o}_{F_\mathfrak{p}}\sqrt{-1}$. A contradiction is derived, so one obtains $ord_\mathfrak{p}(\kappa)$ is even.

Let $ord_\mathfrak{p}(\kappa)=2n$. Since E/F is totally ramified and of degree 2, one can write $\beta=\pi_F^n\mu$, where π_F is a uniformizer of F and $\mu\in\mathfrak{o}_{E_v}^\times$. Then $\sigma(\beta)/\beta=\sigma(\mu)/\mu$. Let $\mathfrak{q}$ be the unique place of $\mathbb{Q}(\sqrt{-1})$ above 2. We have

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4=\left(\frac{\sigma(\mu)/\mu,l}{v}\right)_4=\left(\frac{N_{E_v/F_\mathfrak{p}}(\mu),l}{v}\right)_4\cdot\left(\frac{\mu,l}{v}\right)^{-1}$$
$$=\left(\frac{N_{E_v/\mathbb{Q}_2}(\mu),l}{\mathfrak{q}}\right)_4\cdot\left(\frac{N_{E_v/\mathbb{Q}_2}(\mu),l}{2}\right)^{-1}.$$

Since $\mu\in\mathfrak{o}_{E_v}^\times$ and $E_v=\mathbb{Q}_2(\sqrt{-1},\sqrt{-d})$ with $d\equiv 2 \mod 4$, one has

$$N_{E_v/\mathbb{Q}_2}(\mu)=m^2 \text{ for some } m\in\mathbb{Z}_2^\times.$$

So

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4=\left(\frac{m^2,l}{\mathfrak{q}}\right)_4\cdot 1=\left(\frac{m,l}{\mathfrak{q}}\right)=1.$$

(2) Let $d=2d_0$. Then d_0 is odd. By the argument in (1), we only need to show that there exists a $(x_\mathfrak{p},y_\mathfrak{p})\in\mathfrak{o}_{F_\mathfrak{p}}\times\mathfrak{o}_{F_\mathfrak{p}}$ satisfying $x_\mathfrak{p}^2+y_\mathfrak{p}^2=-1$, such that

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4=1.$$

(i) If $d_0 \equiv 1 \mod 4$, then $x^2 - 2d_0y^2 = -1$ is solvable over $\mathbb{Z}_2$. Choose one solution $(x_0, y_0) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, then we have $x_0^2 + (y_0\sqrt{-2d_0})^2 = -1$. Let

$$x_\mathfrak{p} = x_0 \text{ and } y_\mathfrak{p} = y_0\sqrt{-2d_0}.$$

One obtains

$$\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v}\right)_4 = \left(\frac{x_0 - y_0\sqrt{2d_0}, l}{v}\right)_4 = \left(\frac{-1, l}{\mathfrak{q}}\right)_4 = \left(\frac{\sqrt{-1}, l}{\mathfrak{q}}\right) = 1.$$

Let $s \in \mathbb{Z}_2^\times$ such that $s^2 = l/3$ or $-l/3$. For any $\delta \in E_v^*$ satisfies $N_{E_v/F_\mathfrak{p}}(\delta) = \pm 1$, we have

$$\left(\frac{\delta, l}{v}\right)_4 = \left(\frac{\delta, 3}{v}\right)_4 \cdot \left(\frac{\delta, s}{v}\right) \cdot \left(\frac{\delta, \pm 1}{v}\right)_4 = \left(\frac{\delta, 3}{v}\right)_4 \cdot \left(\frac{\pm 1, s}{\mathfrak{p}}\right) \cdot 1 = \left(\frac{\delta, 3}{v}\right)_4.$$

(ii) If $d_0 \equiv 3 \mod 8$, then $F_\mathfrak{p} = \mathbb{Q}_2(\sqrt{-6})$. Let

$$x_\mathfrak{p} = (1 + 2\sqrt{-6})/5 \text{ and } y_\mathfrak{p} = (2 - \sqrt{-6})/5.$$

Then $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = -1$. One has

$$\begin{aligned}\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v}\right)_4 &= \left(\frac{5^{-1}(1 + 2\sqrt{-1}) + 5^{-1}(2 - \sqrt{-1})\sqrt{-6}, 3}{v}\right)_4 \\ &= \left(\frac{5^{-1}(3 - 4\sqrt{-1}), 3}{\mathfrak{q}}\right)_4 \\ &= \left(\frac{3 - 4\sqrt{-1}, 3}{\mathfrak{q}}\right)_4 \cdot \left(\frac{5, 3}{\mathfrak{q}}\right)_4^{-1}.\end{aligned}$$

It's easy to see

$$\left(\frac{5, 3}{\mathfrak{q}}\right)_4 = \left(\frac{-3, 3}{\mathfrak{q}}\right)_4 = 1.$$

By the class field theory, we have

$$\begin{aligned}\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v}\right)_4 &= \prod_{w|3}\left(\frac{3 - 4\sqrt{-1}, 3}{w}\right)_4 \prod_{w|5}\left(\frac{3 - 4\sqrt{-1}, 3}{w}\right)_4 \\ &= (-\sqrt{-1})^{(3^2-1)/4} \cdot \left(\frac{5^2, 3}{5}\right)_4 \\ &= (-1) \cdot (-1) = 1,\end{aligned}$$

where w is in the set of places of $\mathbb{Q}(\sqrt{-1})$.

(iii) If $d_0 \equiv 7 \mod 8$, then $F_\mathfrak{p} = \mathbb{Q}_2(\sqrt{-14})$. Let

$$x_\mathfrak{p} = (3 - 2\sqrt{-14})/13 \text{ and } y_\mathfrak{p} = (2 + 3\sqrt{-14})/13.$$

Then $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = -1$. One has

$$\begin{aligned}\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, l}{v}\right)_4 &= \left(\frac{13^{-1}(3 + 2\sqrt{-1}) + 13^{-1}(-2 + 3\sqrt{-1})\sqrt{-14}, 3}{v}\right)_4 \\ &= \left(\frac{13^{-1}(-5 - 12\sqrt{-1}), 3}{\mathfrak{q}}\right)_4 \\ &= \left(\frac{-5 - 12\sqrt{-1}, 3}{\mathfrak{q}}\right)_4 \cdot \left(\frac{13, 3}{\mathfrak{q}}\right)_4^{-1}.\end{aligned}$$

It's easy to see

$$\left(\frac{13,3}{\mathfrak{q}}\right)_4 = \left(\frac{-3,3}{\mathfrak{q}}\right)_4 = 1.$$

By the class field theory, we have

$$\begin{aligned}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},l}{v}\right)_4 &= \prod_{w|3}\left(\frac{-5-12\sqrt{-1},3}{w}\right)_4 \prod_{w|13}\left(\frac{-5-12\sqrt{-1},3}{w}\right)_4 \\ &= 1\cdot\left(\frac{13^2,3}{13}\right)_4 = 1\cdot 1 = 1,\end{aligned}$$

where w is in the set of places of $\mathbb{Q}(\sqrt{-1})$. □

Remark. In the above three lemmas we don't assume that $d>0$, l prime and $l \mid d$.

Recall

$$D_3 = \{(d,p) \in C | d \equiv 3 \mod 8, p \equiv 5 \mod 8\}.$$

In the following, we give some properties about the case $(d,p) \in D_3$.

Proposition 1.7. *Let $(d,p) \in D_3$ and $F = \mathbb{Q}(\sqrt{-d})$. If $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \pm 1$, then*

$$\prod_{v|p}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},p}{v}\right)_4 = 1$$

where $v \in \Omega_E$ and $\mathfrak{p}$ is the unique place of F above p.

Proof. The Hilbert symbol

$$\begin{aligned}\prod_{v|p}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},p}{v}\right)_4 &= \prod_{v|p}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},-d}{v}\right)_4 \cdot \prod_{v|p}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},-d/p}{v}\right)_4^{-1} \\ &= \prod_{v|p}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},-d}{v}\right)_4 \cdot 1 = \prod_{v|p}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},\sqrt{-d}}{v}\right) \\ &= \left(\frac{\pm 1,p}{p}\right) = 1,\end{aligned}$$

where the second equation holds since $E(\sqrt[4]{-d/p})/E$ is unramified over v. □

Proposition 1.8. *Let $(d,p) \in D_3$ and $F = \mathbb{Q}(\sqrt{-d})$. Let $(x_\mathfrak{p}, y_\mathfrak{p}) \in \mathfrak{o}_{F_\mathfrak{p}} \times \mathfrak{o}_{F_\mathfrak{p}}$, then*

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},p}{v}\right)_4 = \begin{cases} 1 & \text{if } x_\mathfrak{p}^2+y_\mathfrak{p}^2 = 1 \\ -1 & \text{if } x_\mathfrak{p}^2+y_\mathfrak{p}^2 = -1 \end{cases}$$

where v and $\mathfrak{p}$ are respectively the unique place of E and F above 2.

Proof. The Hilbert symbol

$$\begin{aligned}\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},p}{v}\right)_4 &= \left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},\sqrt{p}}{v}\right) = \left(\frac{\pm 1,\sqrt{p}}{\mathfrak{p}}\right) \\ &= \left(\frac{\pm 1,-p}{2}\right) = \pm 1,\end{aligned}$$

where the second equation holds since $F_\mathfrak{p} = \mathbb{Q}_2(\sqrt{-d}) = \mathbb{Q}_2(\sqrt{p})$. □

Now we can prove Theorem 0.3 by using the above propositions.

Proof. Let $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$. Let $\mathfrak{p}$ be a place of F and $L_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of L inside $E_\mathfrak{p} = E \otimes_F F_\mathfrak{p}$. Recall $T = R^1_{E/F}(\mathbb{G}_{m,E})$ and $\mathbf{T}$ is the affine scheme defined by the equation $x^2 + y^2 = 1$, we have

$$T(F) = \{\beta \in E^* : \ N_{E/F}(\beta) = 1\}$$
$$\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}}) = \{\beta \in L_\mathfrak{p}^\times : \ N_{E_\mathfrak{p}/F_\mathfrak{p}}(\beta) = 1\}.$$

And $L_\infty^\times = E_\infty^* = \mathbb{C}^* \times \mathbb{C}^*$.

Let $v \in \Omega_E$ and $v \mid 2$. Let $\mathfrak{p}$ be the unique place of F above 2. By Proposition 1.3 and 1.8, one has

$$\prod_{v|2} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v} \right)_4 = 1$$

for any $(x_\mathfrak{p}, y_\mathfrak{p}) \in \mathfrak{o}_{F_\mathfrak{p}} \times o_{F_\mathfrak{p}}$ with $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = 1$. Regard $\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})$ as a subgroup of $T(\mathbb{A}_F)$, this implies that

$$\lambda_E(\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})) \subseteq E^* N_{\Theta/E}(\mathbb{I}_\Theta).$$

Let $v \in \Omega_E$ and $v \mid p$. Let $\mathfrak{p}$ be the unique place of F above p. By Proposition 1.2 and 1.7, one has

$$\prod_{v|p} \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v} \right)_4 = 1$$

for any $(x_\mathfrak{p}, y_\mathfrak{p}) \in \mathfrak{o}_{F_\mathfrak{p}} \times o_{F_\mathfrak{p}}$ with $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = 1$. This implies that

$$\lambda_E(\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})) \subseteq E^* N_{\Theta/E}(\mathbb{I}_\Theta).$$

And Θ/E is unramified over each place v of E except $v \mid 2p$. Therefore the natural group homomorphism

$$\widetilde{\lambda}_E : {}^{T(\mathbb{A}_F)}\!/_{T(F)\prod_{\mathfrak{p}\le\infty}\mathbf{T}(\mathfrak{o}_{F_\mathfrak{p}})} \longrightarrow \left[{}^{\mathbb{I}_E}\!/_{E^* N_{\Theta/E}(\mathbb{I}_\Theta)}\right] \times \left[{}^{\mathbb{I}_E}\!/_{E^*\prod_{\mathfrak{p}\le\infty} L_\mathfrak{p}^\times}\right]$$

is well-defined. By Proposition 1.1, we only need to show $\widetilde{\lambda}_E$ is injective.

Let $u \in ker\widetilde{\lambda}_E$. Then there are $\beta \in E^*$ and $i \in \prod_{\mathfrak{p}\le\infty} L_\mathfrak{p}^\times$ with $\lambda_E(u) = \beta i$. We have

$$N_{E/F}(\beta) = N_{E/F}(i)^{-1} \in F^* \cap (\prod_{\mathfrak{p}\le\infty} \mathfrak{o}_{F_\mathfrak{p}}^\times) = \{\pm 1\},$$

since F is an imaginary quadratic field and $F \neq \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$.

If $N_{E/F}(\beta) \neq 1$, one obtains $N_{E/F}(\beta) = N_{E/F}(i) = -1$. Write $i = (i_v)_v \in \mathbb{I}_E$. Since Θ/E is unramified over each place v of E except $v \mid 2p$, one concludes that $\psi_{\Theta/E}(i_v)$ is trivial for all primes $v \nmid 2p$, where i_v is regarded as an idele whose v-component is i_v and 1 otherwise.

(1) Suppose $(d, p) \in D_1 \cup D_2$. Since $N_{E/F}(i_v) = -1$ and $i_v \in L_\mathfrak{p}^\times$, one gets

$$\prod_{v|2} \psi_{\Theta/E}(i_v) = 1 \text{ and } \psi_{\Theta/E}(i_{v'}) = -1$$

by Proposition 1.2 and 1.3, where $\psi_{\Theta/E} : \mathbb{I}_E \to Gal(\Theta/E)$ is the Artin map and v' is the unique place of E above p. So

$$\psi_{\Theta/E}(\beta i) = \psi_{\Theta/E}(i) = \prod_{v|2} \psi_{\Theta/E}(i_v) \cdot \psi_{\Theta/E}(i_{v'}) = -1.$$

This contradicts to $u \in ker\widetilde{\lambda}_E$.

(2) Suppose $(d,p)\in D_3$. Since $N_{E/F}(i_v)=-1$ and $i_v\in L_{\mathfrak{p}}^{\times}$, one gets

$$\psi_{\Theta/E}(i_{v'})=-1 \text{ and } \prod_{v|p}\psi_{\Theta/E}(i_v)=1$$

by Proposition 1.7 and 1.8, where v' is the unique place of E above 2. So

$$\psi_{\Theta/E}(\beta i)=\psi_{\Theta/E}(i)=\psi_{\Theta/E}(i_{v'})\cdot\prod_{v|p}\psi_{\Theta/E}(i_v)=-1.$$

This contradicts to $u\in ker\widetilde{\lambda}_E$.

Therefore $N_{E/F}(\beta)=1$, one concludes that

$$N_{E/F}(\beta)=N_{E/F}(i)=1 \quad\Rightarrow\quad \beta\in T(F) \quad\text{and}\quad i\in\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}).$$

So $\beta i\in T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$. Then $\widetilde{\lambda}_E$ is injective. □

Lemma 1.9. *Let $F=\mathbb{Q}(\sqrt{-2d})$ and $d\equiv 3 \mod 4$. If $x_{\mathfrak{p}}$ and $y_{\mathfrak{p}}$ in $\mathfrak{o}_{F_{\mathfrak{p}}}$ satisfy $x_{\mathfrak{p}}^2+y_{\mathfrak{p}}^2=-1$, then the 4-th Hilbert symbol*

$$\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},2}{v}\right)_4=-1$$

where v and $\mathfrak{p}$ are respectively the unique place of E and F above 2.

Proof. The Hilbert symbol

$$\begin{aligned}\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},2}{v}\right)_4&=\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},-2d}{v}\right)_4\cdot\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},-d}{v}\right)_4^{-1}\\&=\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},-2d}{v}\right)_4\cdot 1=\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},\sqrt{-2d}}{v}\right)\\&=\left(\frac{-1,2d}{2}\right)=-1\end{aligned}$$

where the second equation holds by Lemma 1.6. □

Using a similar argument as in the proof of Theorem 0.3, the result follows from Lemma 1.6 and 1.9.

Proposition 1.10. *Let $F=\mathbb{Q}(\sqrt{-2d})$ and $d\equiv 3 \mod 4$. Then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of Θ and H_L, where $\Theta=E(\sqrt[4]{2})$ and H_L is the ring class field corresponding to the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$.*

Now we use Proposition 1.10 to give an explicit example. Let $F=\mathbb{Q}(\sqrt{-6})$. We write $N_{F/\mathbb{Q}}(\alpha)=2^{s_1}3^{s_2}p_1^{e_1}\cdots p_g^{e_g}$ for any $\alpha=a+b\sqrt{-6}$ and $a,b\in\mathbb{Z}$. Let $P(n)=\{p_1,\cdots,p_g\}$. Denote $a=3^{s_3}a_1$ with $3\nmid a_1$ and

$$\begin{aligned}P_1&=\{p\in P(n):\left(\frac{-1}{p}\right)=\left(\frac{-6}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)=-1\}\\P_2&=\{p\in P(n):\left(\frac{-1}{p}\right)=-\left(\frac{-6}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)=-1\}\\P_3&=\{p\in P(n):\left(\frac{-1}{p}\right)=\left(\frac{-6}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)_4=-1\}.\end{aligned}$$

It's easy to see that e_i is even when $p_i\in P_2$.

Example 1.11. *Let $F = \mathbb{Q}(\sqrt{-6})$ and α an integer in F with the above notation. Then $x^2 + y^2 = \alpha$ is solvable over $\mathfrak{o}_F$ if and only if*

(1) The equation $x^2 + y^2 = \alpha$ has integral solutions at every place of F.

(2) $P_1 \neq \emptyset$, or

$$s_1/2 + \sum_{p_i \in P_2} e_i/2 + \sum_{p_i \in P_3} e_i \equiv \begin{cases} 0 \mod 2 & \text{if } a_1 \equiv 1, 3 \mod 8 \\ 1 \mod 2 & \text{if } a_1 \equiv -1, -3 \mod 8 \end{cases}$$

for $P_1 = \emptyset$.

2. The sum of two squares in real quadratic fields

Let $d > 1$ be a square-free odd number and $F = \mathbb{Q}(\sqrt{2d})$. Let $\mathfrak{o}_F$ be the ring of integers of F, ε_F the fundamental unit of $\mathfrak{o}_F$ and $\varepsilon_F = a + b\sqrt{2d}$ with $a, b > 0$. Let $E = F(\sqrt{-1})$. One takes the order $L = \mathfrak{o}_F + \mathfrak{o}_F\sqrt{-1}$ inside E. In this section we always assume that one of the equations $x^2 - 2dy^2 = \pm 2$ is solvable over $\mathbb{Z}$ and we fix one solution (x_0, y_0). Denote $\omega = x_0 + y_0\sqrt{2d}$ and $\eta = \omega^2/2$. Then $\eta \in \mathfrak{o}_F^\times$ and $\eta = \varepsilon_F^{i_0}$ for some $i_0 \in \mathbb{Z}$. By the assumption, we have $N_{F/\mathbb{Q}}(\varepsilon_F) = 1$ (see [16], pp. 106-109).

Lemma 2.1. *Let $p \equiv \pm 3 \mod 8$ and $p|d$. If one of the equations $x^2 - 2dy^2 = \pm 2$ is solvable over $\mathbb{Z}$ with the notation as above, then i_0 is odd and the 4-th Hilbert symbol*

$$\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v}\right)_4 = -1$$

for $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \varepsilon_F$, where v and $\mathfrak{p}$ are respectively the unique prime in E and F above p.

Proof. The Hilbert symbol

$$\begin{aligned}\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v}\right)_4 &= \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, 2d}{v}\right)_4 \cdot \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, 2d/p}{v}\right)_4^{-1} \\ &= \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, 2d}{v}\right)_4 \cdot 1 = \left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, \sqrt{2d}}{v}\right) \\ &= \left(\frac{\varepsilon_F, \sqrt{2d}}{\mathfrak{p}}\right)\end{aligned}$$

where the second equation holds since $E(\sqrt[4]{2d/p})/E$ is unramified over v. However,

$$\left(\frac{\eta, \sqrt{2d}}{\mathfrak{p}}\right) = \left(\frac{\omega^2/2, \sqrt{2d}}{\mathfrak{p}}\right) = \left(\frac{2, p}{p}\right) = -1.$$

Then

$$-1 = \left(\frac{\eta, \sqrt{2d}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_F, \sqrt{2d}}{\mathfrak{p}}\right)^{i_0}.$$

Therefore $\left(\frac{\varepsilon_F, \sqrt{2d}}{\mathfrak{p}}\right) = -1$ and i_0 is odd. □

Lemma 2.2. *Let $p|d$, $p \equiv \pm 3 \mod 8$. And one of the equations $x^2 - 2dy^2 = \pm 2$ is solvable over $\mathbb{Z}$ with the notation as above. If $x_\mathfrak{p}$ and $y_\mathfrak{p}$ in $\mathfrak{o}_{F_\mathfrak{p}}$ satisfy $x_\mathfrak{p}^2 + y_\mathfrak{p}^2 = \varepsilon_F$, then*

$$\left(\frac{x_\mathfrak{p} + y_\mathfrak{p}\sqrt{-1}, p}{v}\right)_4 = 1$$

where v and $\mathfrak{p}$ are respectively the unique place of E and F above 2.

Proof. Since $E_v = F_\mathfrak{p}(\sqrt{-1})$ is ramified over $F_\mathfrak{p}$, there is a uniformizer π_F in $F_\mathfrak{p}$ such that $\left(\frac{\pi_F,-1}{\mathfrak{p}}\right) = 1$. We know $x^2+y^2 = \pi_F^3$ is solvable over $\mathfrak{o}_{F_\mathfrak{p}}$ and $x^2+y^2 = \pi_F$ is not solvable over $\mathfrak{o}_{F_\mathfrak{p}}$ (by Theorem 1 in [6]). Choose (a,b) be one solution of the equation $x^2+y^2 = \pi_F^3$, then we have a and $b \in \mathfrak{o}_{F_\mathfrak{p}}^\times$, otherwise we obtains $x^2+y^2 = \pi_F$ is solvable over $\mathfrak{o}_{F_\mathfrak{p}}$.

Recall $\omega = x_0 + y_0\sqrt{2d}$ and $\eta = \omega^2/2$, here $x_0, y_0 \in \mathbb{Z}$ satisfy $x_0^2 - 2dy_0^2 = \pm 2$. Denote

$$\epsilon = 2^{-1}\omega\cdot(1+\sqrt{-1})\cdot(a+b\sqrt{-1})/(a-b\sqrt{-1}).$$

We can see $N_{E_v/F_\mathfrak{p}}(\epsilon) = \eta$. And

$$\begin{aligned}\epsilon &= 2^{-1}\pi_F^{-3}\omega\cdot(1+\sqrt{-1})\cdot(a^2-b^2+2ab\sqrt{-1})\\ &= 2^{-1}\pi_F^{-3}\omega\cdot[(a^2-b^2-2ab)+(a^2-b^2+2ab)\sqrt{-1}]\\ &= (\omega/2 - b\omega(a+b)/\pi_F^3) + (\omega/2 - b\omega(b-a)/\pi_F^3)\sqrt{-1}.\end{aligned}$$

In the following we will prove $a \not\equiv \pm b \mod 2$. If not then $a = \pm b + 2u$ for some $u \in \mathfrak{o}_{F_\mathfrak{p}}$. We have $(\pm b+2u)^2 + b^2 = \pi_F^3$. Note that $b \in \mathfrak{o}_{F_\mathfrak{p}}^\times$, then

$$2 = ord_\mathfrak{p}(4u^2+2b^2\pm 4ub) = ord_\mathfrak{p}(\pi_F^3) = 3,$$

a contradiction is derived. So $a \not\equiv b \mod 2$. Since a, b are units and the residue field of $\mathfrak{o}_{F_\mathfrak{p}}$ is $\mathbb{F}_2$, we have

$$a+b = \pi_F u_1, a-b = \pi_F u_2$$

with $u_1, u_2 \in \mathfrak{o}_{F_\mathfrak{p}}^\times$. Then

$$\begin{aligned}\epsilon &= (\omega/2 - bu_1\omega/\pi_F^2) + \sqrt{-1}(\omega/2 + bu_2\omega/\pi_F^2)\\ &= 2^{-1}\omega(1 - bu_1\frac{2}{\pi_F^2}) + 2^{-1}\omega(1+bu_2\frac{2}{\pi_F^2})\sqrt{-1}.\end{aligned}$$

We have $\epsilon \in \mathfrak{o}_{F_\mathfrak{p}} + \mathfrak{o}_{F_\mathfrak{p}}\sqrt{-1}$ since $b, u_1, u_2 \in \mathfrak{o}_{F_\mathfrak{p}}^\times$ and the residue field of $\mathfrak{o}_{F_\mathfrak{p}}$ is $\mathbb{F}_2$.

Let $\mathfrak{q}$ be the unique prime of $\mathbb{Q}(\sqrt{-1})$ above 2. Let $s \in \mathbb{Z}_2^\times$ such that $s^2 = p/3$ or $-p/3$. For any $\delta \in E_v^*$ satisfies $N_{E_v/F_\mathfrak{p}}(\delta) = \eta$, we have

$$\begin{aligned}\left(\frac{\delta,p}{v}\right)_4 &= \left(\frac{\delta,3}{v}\right)_4\cdot\left(\frac{\delta,s}{v}\right)\cdot\left(\frac{\delta,\pm 1}{v}\right)_4 = \left(\frac{\delta,3}{v}\right)_4\cdot\left(\frac{\eta,s}{\mathfrak{p}}\right)\cdot 1\\ &= \left(\frac{\delta,3}{v}\right)_4\cdot\left(\frac{1,s}{p}\right) = \left(\frac{\delta,3}{v}\right)_4.\end{aligned}$$

Then

$$\begin{aligned}\left(\frac{\epsilon,p}{v}\right)_4 &= \left(\frac{2^{-1}\pi_F^{-3}\omega\cdot(1+\sqrt{-1})\cdot(a+b\sqrt{-1})^2,3}{v}\right)_4\\ &= \left(\frac{2^{-1},3}{v}\right)_4\cdot\left(\frac{\pi_F^3,3}{v}\right)_4^{-1}\cdot\left(\frac{\omega,3}{v}\right)_4\cdot\left(\frac{1+\sqrt{-1},3}{v}\right)_4\cdot\left(\frac{a+b\sqrt{-1},3}{v}\right)\\ &= \left(\frac{2^{-1},3}{\mathfrak{q}}\right)\cdot\left(\frac{\pi_F^3,3}{v}\right)_4^{-1}\cdot\left(\frac{\pm 2,3}{\mathfrak{q}}\right)_4\cdot\left(\frac{1+\sqrt{-1},3}{\mathfrak{q}}\right)\cdot\left(\frac{\pi_F^3,3}{\mathfrak{p}}\right)\\ &= 1\cdot\left(\frac{\pi_F^3,3}{v}\right)_4^{-1}\cdot 1\cdot(-1)\cdot\left(\frac{\pi_F,3}{\mathfrak{p}}\right)\end{aligned}$$

Since $\left(\frac{\pi_F,-1}{\mathfrak{p}}\right)=1$ by the choice of π_F and $F_{\mathfrak{p}}(\sqrt{-3})/F_{\mathfrak{p}}$ is unramifed of degree 2, then one obtains

$$\left(\frac{\pi_F,3}{\mathfrak{p}}\right)=\left(\frac{\pi_F,-3}{\mathfrak{p}}\right)=-1.$$

Therefore

$$\left(\frac{\epsilon,p}{v}\right)_4=\left(\frac{\pi_F^3,3}{v}\right)_4^{-1}=\left(\frac{N_{E_v/\mathbb{Q}_2}(a+b\sqrt{-1}),3}{\mathfrak{q}}\right)_4^{-1}.$$

We can write $N_{E_v/\mathbb{Q}_2}(a+b\sqrt{-1})=2^3m$ with $m\equiv 1$ or $-3 \mod 8$. Therefore

$$\begin{aligned}\left(\frac{\epsilon,p}{v}\right)_4&=\left(\frac{2^3m,3}{\mathfrak{q}}\right)_4^{-1}=\left(\frac{m,3}{\mathfrak{q}}\right)_4^{-1}\\&=\begin{cases}1 & \text{if } m\equiv 1 \mod 8\\ \left(\frac{-3,3}{\mathfrak{q}}\right)_4^{-1}=1 & \text{if } m\equiv -3 \mod 8.\end{cases}\end{aligned}$$

Let $x_{\mathfrak{p}}$ and $y_{\mathfrak{p}}$ in $\mathfrak{o}_{F_{\mathfrak{p}}}$ satisfy $x_{\mathfrak{p}}^2+y_{\mathfrak{p}}^2=\varepsilon_F$. Since $\eta=\varepsilon_F^{i_0}$, we have

$$\left(\frac{\epsilon,p}{v}\right)_4=\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},p}{v}\right)_4^{i_0}$$

by Lemma 1.6. Since i_0 is odd by Lemma 2.1, one obtains

$$\left(\frac{x_{\mathfrak{p}}+y_{\mathfrak{p}}\sqrt{-1},p}{v}\right)_4=1.$$

□

Corollary 2.3. *Let $F=\mathbb{Q}(\sqrt{2d})$ and $p|d$, $p\equiv\pm 3 \mod 8$. If one of the equations $x^2-2dy^2=\pm 2$ is solvable over $\mathbb{Z}$, then $x^2+y^2=\varepsilon_F$ is not solvable over $\mathfrak{o}_F$.*

Proof. Recall $\mathbf{X}_{\varepsilon_F}$ is the affine scheme over $\mathfrak{o}_F$ defined by $x^2+y^2=\varepsilon_F$. Let $\Theta=E(\sqrt[4]{p})$. One obtains

$$\psi_{\Theta/E}(f_E[\prod_{\mathfrak{p}\le\infty}(x_{\mathfrak{p}},y_{\mathfrak{p}})])=\left(\frac{x_{\mathfrak{p}'}+y_{\mathfrak{p}'}\sqrt{-1},p}{v}\right)_4=-1$$

for any $\prod_{\mathfrak{p}\le\infty}(x_{\mathfrak{p}},y_{\mathfrak{p}})\in\prod_{\mathfrak{p}\le\infty}\mathbf{X}_{\varepsilon_F}(\mathfrak{o}_{F_{\mathfrak{p}}})$ by Lemma 2.1 and 2.2, where $\psi_{\Theta/E}$ is the Artin map, v and $\mathfrak{p}'$ are respectively the unique prime of E and F above p . The result follows from the class field theory. □

Remark. In fact $x^2+y^2=\varepsilon_F$ has local integral solutions at every place of F. The solvability is obvious if the place is not above 2. Let $\mathfrak{p}$ be the unique place of F above 2. Then we only need to show that it is solvable over $\mathfrak{o}_{F_{\mathfrak{p}}}$. Since $\eta=\omega^2/2=\varepsilon_F^{i_0}$ with i_0 odd, we have

$$x^2+y^2=\varepsilon_F \text{ is solvable over } \mathfrak{o}_{F_{\mathfrak{p}}} \Leftrightarrow x^2+y^2=\eta \text{ is solvable over } \mathfrak{o}_{F_{\mathfrak{p}}}.$$

Note that $\omega=x_0+y_0\sqrt{2d}$ with $2\mid x_0$ and y_0 odd. It is easy to verify that $x^2+y^2=\eta$ is solvable over $\mathfrak{o}_{F_{\mathfrak{p}}}$ by Theorem 1 in [6].

Theorem 2.4. *Let $F=\mathbb{Q}(\sqrt{2d})$. If $p|d$, $p\equiv\pm 3 \mod 8$ and one of the equations $x^2-2dy^2=\pm 2$ is solvable over $\mathbb{Z}$, then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of Θ and H_L, where $\Theta=E(\sqrt[4]{p})$ and H_L is the ring class field corresponding to the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$.*

Proof. Let $\mathfrak{p}$ be a place of F and $L_{\mathfrak{p}}$ the $\mathfrak{p}$-adic completion of L inside $E_{\mathfrak{p}} = E \otimes_F F_{\mathfrak{p}}$.

Let v_1 and $\mathfrak{p}_1$ be respectively the unique prime of E and F above 2. By Lemma 1.6, one has $\left(\frac{\xi, p}{v}\right)_4 = 1$ for any $\xi \in L_{\mathfrak{p}_1}^{\times}$ with $N_{E_{v_1}/F_{\mathfrak{p}_1}}(\xi) = 1$. This implies that

$$\lambda_E(\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}_1}})) \subseteq N_{\Theta_{\mathfrak{V}_1}/E_{v_1}}(\Theta_{\mathfrak{V}_1}^*)$$

where $\mathfrak{V}_1$ is the unique place of Θ above v_1.

Let v_2 and $\mathfrak{p}_2$ be respectively the unique prime of E and F above p. By the similar computation in Lemma 2.1, one has $\left(\frac{\xi, p}{v}\right)_4 = 1$ for any $\xi \in L_{\mathfrak{p}_2}^{\times}$ with $N_{E_{v_2}/F_{\mathfrak{p}_2}}(\xi) = 1$. This implies that

$$\lambda_E(\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}_2}})) \subseteq N_{\Theta_{v_2}/E_{v_2}}(\Theta_{v_2}^*)$$

where $\Theta_{v_2} = \Theta \otimes_E E_{v_2}$.

Since Θ/E is unramified over all primes except v_1 and v_2, therefore the natural group homomorphism

$$\widetilde{\lambda}_E : {}^{T(\mathbb{A}_F)}\!/_{T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})} \longrightarrow \left[{}^{\mathbb{I}_E}\!/_{E^* N_{\Theta/E}(\mathbb{I}_\Theta)}\right] \times \left[{}^{\mathbb{I}_E}\!/_{E^* \prod_{\mathfrak{p}\leq\infty} L_{\mathfrak{p}}^{\times}}\right]$$

is well-defined. By Proposition 1.1, we only need to show $\widetilde{\lambda}_E$ is injective.

Let $u \in ker\widetilde{\lambda}_E$. Then there are $\beta \in E^*$ and $i \in \prod_{\mathfrak{p}\leq\infty} L_{\mathfrak{p}}^{\times}$ with $\widetilde{\lambda}_E(u) = \beta i$. Therefore

$$N_{E/F}(\beta) = N_{E/F}(i)^{-1} \in F^* \cap \Big(\prod_{\mathfrak{p}\leq\infty} \mathfrak{o}_{F_{\mathfrak{p}}}^{\times}\Big) = \{\pm\varepsilon_F^n | n \in \mathbb{Z}\}.$$

Since $N_{E/F}(\beta)$ is totally positive, we have $N_{E/F}(\beta) = \varepsilon_F^n$ and $N_{E/F}(i) = \varepsilon_F^{-n}$.

Assume that n is odd. Write $i = (i_v)_v \in \mathbb{I}_E$. Since Θ/E is unramified over all primes of E except v_1 and v_2, one has $\psi_{\Theta/E}(i_v)$ is trivial for all primes $v \neq v_1, v_2$, where i_v is regarded as an idele whose v-component is i_v and 1 otherwise. Since $N_{E_v/F_{\mathfrak{p}}}(i_v) = \varepsilon_F^{-n}$, one gets

$$\psi_{\Theta/E}(\beta i) = \psi_{\Theta/E}(i) = \psi_{\Theta/E}(i_{v_1})\psi_{\Theta/E}(i_{v_2}) = 1 \cdot (-1)^{-n} = -1$$

by Lemma 2.1 and 2.2, where $\psi_{\Theta/E}$ is the Artin map. This contradicts to $u \in ker\widetilde{\lambda}_E$.

Therefore n is even. Let

$$\gamma = \beta\varepsilon_F^{n/2}, j = i\varepsilon_F^{-n/2}.$$

Then

$$N_{E/F}(\gamma) = N_{E/F}(j) = 1 \quad \Rightarrow \quad \gamma \in T(F) \quad \text{and} \quad j \in \prod_{\mathfrak{p}\leq\infty} \mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}}).$$

So $\beta i = \gamma j \in T(F)\prod_{\mathfrak{p}\leq\infty}\mathbf{T}(\mathfrak{o}_{F_{\mathfrak{p}}})$. Then $\widetilde{\lambda}_E$ is injective. □

In the following we consider a special case. Let $d = p$ be a prime with $p \equiv 3 \mod 8$. Then the equation $x^2 - 2py^2 = -2$ is solvable over $\mathbb{Z}$ (Corollary 2 in [19]).

Lemma 2.5. *Let $F = \mathbb{Q}(\sqrt{2p})$ and $p \equiv 3 \mod 8$. If $x_{\mathfrak{p}}$ and $y_{\mathfrak{p}}$ in $\mathfrak{o}_{F_{\mathfrak{p}}}$ satisfy $x_{\mathfrak{p}}^2 + y_{\mathfrak{p}}^2 = \varepsilon_F$, then the 4-th Hilbert symbol*

$$\left(\frac{x_{\mathfrak{p}} + y_{\mathfrak{p}}\sqrt{-1}, 2}{v}\right)_4 = -1$$

where v and $\mathfrak{p}$ are respectively the unique prime in E and F above 2.

Proof. The Hilbert symbol

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},2}{v}\right)_4=\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},2p}{v}\right)_4\cdot\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},p}{v}\right)_4^{-1}$$
$$=\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},\sqrt{2p}}{v}\right)\cdot 1=\left(\frac{\varepsilon_F,\sqrt{2p}}{\mathfrak{p}}\right)$$

where the second equation holds by Lemma 2.2. Recall $\omega=x_0+y_0\sqrt{2d}$ and $\eta=\omega^2/2$, here $x_0,y_0\in\mathbb{Z}$ satisfy $x_0^2-2py_0^2=-2$. And $\eta=\varepsilon_F^{i_0}$ for some $i_0\in\mathbb{Z}$. By Lemma 2.1, we have i_0 is odd. So we have

$$\left(\frac{x_\mathfrak{p}+y_\mathfrak{p}\sqrt{-1},2}{v}\right)_4=\left(\frac{\varepsilon_F,\sqrt{2p}}{\mathfrak{p}}\right)=\left(\frac{\omega^2/2,\sqrt{2p}}{\mathfrak{p}}\right)$$
$$=\left(\frac{2,\sqrt{2p}}{\mathfrak{p}}\right)=\left(\frac{2,-2p}{2}\right)=-1.$$

□

Using a similar argument as in the proof of Theorem 2.4, the result follows from Lemma 2.2 and 2.5.

Proposition 2.6. *Let p be a prime and $F=\mathbb{Q}(\sqrt{2p})$. If $p\equiv 3 \mod 8$, then the diophantine equation $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if α satisfies the Artin condition of Θ and H_L, where $\Theta=E(\sqrt[4]{2})$ and H_L is the ring class field corresponding to the order $L=\mathfrak{o}_F+\mathfrak{o}_F\sqrt{-1}$.*

Now we use Theorem 2.6 to give an explicit example. Let $F=\mathbb{Q}(\sqrt{6})$. We write $N_{F/\mathbb{Q}}(\alpha)=2^{s_1}3^{s_2}p_1^{e_1}\cdots p_g^{e_g}$ for any $\alpha=a+b\sqrt{6}$, here $a,b\in\mathbb{Z}$. Let $P(n)=\{p_1,\cdots,p_g\}$. Denote $a=3^{s_3}a_1$ with $3\nmid a_1$ and

$$P_1=\{p\in P(n):\left(\frac{-1}{p}\right)=\left(\frac{6}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)=-1\}$$
$$P_2=\{p\in P(n):\left(\frac{-1}{p}\right)=-\left(\frac{6}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)=-1\}$$
$$P_3=\{p\in P(n):\left(\frac{-1}{p}\right)=\left(\frac{6}{p}\right)=1 \text{ and } \left(\frac{2}{p}\right)_4=-1\}.$$

It's easy to see that e_i is even when $p_i\in P_2$.

Example 2.7. *Let $F=\mathbb{Q}(\sqrt{6})$ and α an integer in F with the above notation. Then $x^2+y^2=\alpha$ is solvable over $\mathfrak{o}_F$ if and only if*

(1) The equation $x^2+y^2=\alpha$ has integral solutions at every place of F.

(2) $P_1\neq\emptyset$, or

$$s_1/2+\sum_{p_i\in P_2}e_i/2+\sum_{p_i\in P_3}e_i\equiv\begin{cases}0 \mod 2 & \text{if } a_1\equiv\pm1 \mod 8\\ 1 \mod 2 & \text{if } a_1\equiv\pm3 \mod 8\end{cases}$$

for $P_1=\emptyset$.

Acknowledgment *The work is supported by the Morningside Center of Mathematics and NSFC, grant # 10901150 and # 10671104.*

References

[1] D.A.Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley & Sons, Inc., 1989.

[2] J-L.Colliot-Thélène and F. Xu, *Brauer-Manin obstruction for integral points of homogeneous spaces and representations by integral quadratic forms*, Compositio Math. **145** (2009), 309–363.

[3] G.L.Dirichlet, *Einige neue Sätze über unbestimmte gleichungen*, "Werke" **I** (1920), 221–236.

[4] P.Epstein, *Zur auflösbarkeit der gleichung $x^2 - Dy^2 = -1$*, J. reine und angew. Math. **171** (1934), 243 –252.

[5] D. Harari, *Le défaut d'approximation forte pour les groups algébriques commutatifs*, Algebra and Number Theory **2** (2008), no. 5, 595–611.

[6] O. Körner, *Integral representations over local fields and the number of genera of quadratic forms*, Acta Arith. **24** (1973), 301–311.

[7] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, 1986.

[8] ———, *Algebraic geometry*, World Scientific Publishing Co., 1998.

[9] T. Nagell, *On the representations of integers as the sum of two integral squares in algebraic, mainly quadratic fields*, Nova Acta Soc. Sci. Upsal. (4) **15** (1953), no. 11, 77pp.

[10] ———, *On the sum of two integral squares in certain quadratic fields*, Ark. Mat. **4** (1961), 267–286.

[11] J.Neukirch, A.Schmidt, and K.Wingberg, *Cohomology of number fields*, Grundlehren, vol. 323, Springer, 2000.

[12] I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. **48** (1940), no. 3, 405–417.

[13] O.T.O'Meara, *Introduction to quadratic forms*, Springer -Verlag, 1973.

[14] M. Peters, *Die stufe von ordnungen ganzer zahlen in algebraischen zahlkörpern*, Math.Ann. **195** (1972), 309–314.

[15] V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory*, Academic Press, 1994.

[16] O. Perron, *Die lehre von den kettenbruchen*, Chelsea Publishing Co., 1929.

[17] L.Rédei, *Über die Pellsche gleichung $t^2 - du^2 = -1$*, J. reine und angew. Math. **173** (1935), 193 –221.

[18] A. N. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001.

[19] H. Yokoi, *Solvability of Diophantine equation $x^2 - Dy^2 = \pm 2$ and new invariants for real quadratic fields*, Nagoya Math. J. **134** (1994), 137 –149.

[20] D. Wei, *On the sum of two integral squares in quadratic fields $\mathbb{Q}(\sqrt{\pm p})$*, Acta Arith. (to appear), arXiv:1004.2996.

[21] D. Wei and F. Xu, *Integral points for multi-norm tori*, arXiv:1004.2608.

[22] ———, *Integral points for groups of multiplicative Type*, arXiv:1004.2613.

Academy of Mathematics and System Science, CAS, Beijing 100190, P.R.China
E-mail address: dshwei@amss.ac.cn